Searchreport & Interference Search

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	6619	713/201	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:37
L2	6619	713/201 or 726/24 or 726/25	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:37
L3	5	726/24 or 726/25	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:37
L4	274	713/188	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:37
L5	93	2 and 4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:38
L6	0	"malicious.clm" and code.clm. and detection.clm. and fastest.clm. and probability.clm. and analyzing.clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:39
L7	0	"malicious.clm" and code.clm. and detection.clm. and fastest.clm. and probability.clm. and analyzing.clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:39
L8	0	malicious.clm. and code.clm. and detection.clm. and fastest.clm. and probability.clm. and analyzing.clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:39

L9	0	"malicious code".clm. and code. clm. and detection.clm. and fastest.clm. and probability.clm. and analyzing.clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:40
L10	1	"malicious code" and code and detection and fastest and probability and analyzing	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/24 20:41

Terms used malicious code and code and detection and fastest and probability and analyzing

Found **37,137** of **169,866**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown Relevance scale □▬▬▬■

1 Pioneer: verifying code integrity and enforcing untampered code execution on legacy systems

Arvind Seshadri, Mark Luk, Elaine Shi, Adrian Perrig, Leendert van Doorn, Pradeep Khosla

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(264.30 KB) Additional Information: full citation, abstract, references, index terms

We propose a primitive, called Pioneer, as a first step towards verifiable code execution on untrusted legacy hosts. Pioneer does not require any hardware support such as secure co-processors or CPU-architecture extensions. We implement Pioneer on an Intel Pentium IV Xeon processor. Pioneer can be used as a basic building block to build security systems. We demonstrate this by building a kernel rootkit detector.

Keywords: dynamic root of trust, rootkit detection, self-check-summing code, software-based code attestation, verifiable code execution

2 Session 2: The top speed of flash worms

Stuart Staniford, David Moore, Vern Paxson, Nicholas Weaver

October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**

Publisher: ACM Press

Full text available: pdf(365.68 KB) Additional Information: full citation, abstract, references, index terms

Flash worms follow a precomputed spread tree using prior knowledge of all systems vulnerable to the worm's exploit. In previous work we suggested that a flash worm could saturate one million vulnerable hosts on the Internet in under 30 seconds[18]. We grossly over-estimated.

In this paper, we revisit the problem in the context of single packet UDP worms (inspired by Slammer and Witty). Simulating a flash version of Slammer, calibrated by current Internet latency measurements and observ ...

Keywords: flash worm, modeling, simulation, worms

3 Vigilante: end-to-end containment of internet worms

Manuel Costa, Jon Crowcroft, Miguel Castro, Antony Rowstron, Lidong Zhou, Lintao Zhang, Paul Barham

October 2005 **ACM SIGOPS Operating Systems Review , Proceedings of the twentieth ACM symposium on Operating systems principles SOSP '05**, Volume 39 Issue 5

Publisher: ACM Press

Full text available: pdf(329.29 KB) Additional Information: full citation, abstract, references, index terms

Worm containment must be automatic because worms can spread too fast for humans to respond. Recent work has proposed network-level techniques to automate worm containment; these techniques have limitations because there is no information about the vulnerabilities exploited by worms at the network level. We propose Vigilante, a new end-to-end approach to contain worms automatically that addresses these limitations. Vigilante relies on collaborative worm detection at end hosts, but does not requir ...

Keywords: control flow analysis, data flow analysis, self-certifying alerts, worm containment

4 Session 4: WORM vs. WORM: preliminary study of an active counter-attack mechanism

Frank Castaneda, Emre Can Sezer, Jun Xu

October 2004 **Proceedings of the 2004 ACM workshop on Rapid malcode**

Publisher: ACM Press

Full text available: pdf(289.95 KB) Additional Information: full citation, abstract, references, index terms

Self-propagating computer worms have been terrorizing the Internet for the last several years. With the increasing density, inter-connectivity and bandwidth of the Internet combined with security measures that inadequately scale, worms will continue to plague the Internet community. Existing anti-virus and intrusion detection systems are clearly inadequate to defend against many recent fast-spreading worms. In this paper we explore an active counter-attack method - anti-worms. We propose a me ...

Keywords: anti-worm, good worm, worm

5 Intrusion detection: Anomaly detection of web-based attacks

Christopher Kruegel, Giovanni Vigna

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Publisher: ACM Press

Full text available: pdf(252.97 KB) Additional Information: full citation, abstract, references, citings, index terms

Web-based vulnerabilities represent a substantial portion of the security exposures of computer networks. In order to detect known web-based attacks, misuse detection systems are equipped with a large number of signatures. Unfortunately, it is difficult to keep up with the daily disclosure of web-related vulnerabilities, and, in addition, vulnerabilities may be introduced by installation-specific web-based applications. Therefore, misuse detection systems should be complemented with anomaly dete ...

Keywords: anomaly detection, network security, world-wide web

6 Fast detection of communication patterns in distributed executions

Thomas Kunz, Michiel F. H. Seuren

November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research**
Publisher: IBM Press
Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

7 Industry/government track papers: Learning to detect malicious executables in the wild
Jeremy Z. Kolter, Marcus A. Maloof
August 2004 **Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining KDD '04**
Publisher: ACM Press
Full text available: pdf(216.52 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we describe the development of a fielded application for detecting malicious executables in the wild. We gathered 1971 benign and 1651 malicious executables and encoded each as a training example using n-grams of byte codes as features. Such processing resulted in more than 255 million distinct n-grams. After selecting the most relevant n-grams for prediction, we evaluated a variety of inductive methods, including naive Bayes, decision trees, support vector machines, and boosting. ...

Keywords: concept learning, data mining, malicious software, security

8 Level set and PDE methods for computer graphics
David Breen, Ron Fedkiw, Ken Museth, Stanley Osher, Guillermo Sapiro, Ross Whitaker
August 2004 **Proceedings of the conference on SIGGRAPH 2004 course notes GRAPH '04**
Publisher: ACM Press
Full text available: pdf(17.07 MB) Additional Information: full citation, abstract

Level set methods, an important class of partial differential equation (PDE) methods, define dynamic surfaces implicitly as the level set (iso-surface) of a sampled, evolving nD function. The course begins with preparatory material that introduces the concept of using partial differential equations to solve problems in computer graphics, geometric modeling and computer vision. This will include the structure and behavior of several different types of differential equations, e.g. the level set eq ...

9 A guided tour to approximate string matching
Gonzalo Navarro
March 2001 **ACM Computing Surveys (CSUR)**, Volume 33 Issue 1
Publisher: ACM Press
Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We survey the current techniques to cope with the problem of string matching that allows errors. This is becoming a more and more relevant issue for many fast growing areas such as information retrieval and computational biology. We focus on online searching and mostly on edit distance, explaining the problem and its relevance, its statistical behavior, its history and current developments, and the central ideas of the algorithms and their complexities. We present a number of experiments to ...

Keywords: Levenshtein distance, edit distance, online string matching, text searching allowing errors

10 Data integrity: Web application security assessment by fault injection and behavior monitoring
Yao-Wen Huang, Shih-Kun Huang, Tsung-Po Lin, Chung-Hung Tsai
May 2003 **Proceedings of the 12th international conference on World Wide Web**
Publisher: ACM Press
Full text available: pdf(4.53 MB) Additional Information: full citation, abstract, references, citings, index terms

As a large and complex application platform, the World Wide Web is capable of delivering a broad range of sophisticated applications. However, many Web applications go through rapid development phases with extremely short turnaround time, making it difficult to eliminate vulnerabilities. Here we analyze the design of Web application security assessment mechanisms in order to identify poor coding practices that render Web applications vulnerable to attacks such as SQL injection and cross-site scr ...

Keywords: black-box testing, complete crawling, fault injection, security assessment, web application testing

11 Safely executing untrusted code: Model-carrying code: a practical approach for safe execution of untrusted applications
R. Sekar, V.N. Venkatakrishnan, Samik Basu, Sandeep Bhatkar, Daniel C. DuVarney
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Publisher: ACM Press
Full text available: pdf(301.30 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents a new approach called *model-carrying code* (MCC) for safe execution of untrusted code. At the heart of MCC is the idea that untrusted code comes equipped with a concise high-level model of its security-relevant behavior. This model helps bridge the gap between high-level security policies and low-level binary code, thereby enabling analyses which would otherwise be impractical. For instance, users can use a fully automated verification procedure to determine if the code ...

Keywords: mobile code security, policy enforcement, sand-boxing, security policies

12 The monitoring and early detection of internet worms
Cliff C. Zou, Weibo Gong, Don Towsley, Lixin Gao
October 2005 **IEEE/ACM Transactions on Networking (TON)**, Volume 13 Issue 5
Publisher: IEEE Press
Full text available: pdf(594.79 KB) Additional Information: full citation, abstract, references, index terms

After many Internet-scale worm incidents in recent years, it is clear that a simple self-propagating worm can quickly spread across the Internet and cause severe damage to our society. Facing this great security threat, we need to build an early detection system that can detect the presence of a worm in the Internet as quickly as possible in order to give people accurate early warning information and possible reaction time for counteractions. This paper first presents an Internet worm monitoring ...

Keywords: computer network security, early detection, internet worm, network monitoring

13 Frontmatter (TOC, Letters, Philosophy of computer science, Interviewers needed, Taking software requirements creation from folklore to analysis, SW components and product lines: from business to systems and technology, Software engineering survey)
September 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 5
Publisher: ACM Press
Full text available: pdf(1.98 MB) Additional Information: full citation

14 Experimental analysis of the fastest optimum cycle ratio and mean algorithms
Ali Dasdan
October 2004 **ACM Transactions on Design Automation of Electronic Systems (TODAES)**, Volume 9 Issue 4
Publisher: ACM Press
Full text available: pdf(464.90 KB) Additional Information: full citation, abstract, references, index terms

Optimum cycle ratio (OCR) algorithms are fundamental to the performance analysis of (digital or manufacturing) systems with cycles. Some applications in the computer-aided design field include cycle time and slack optimization for circuits, retiming, timing separation analysis, and rate analysis. There are many OCR algorithms, and since a superior time complexity in theory does not mean a superior time complexity in practice, or vice-versa, it is important to know how these algorithms perform ...

Keywords: Cycle mean, cycle period, cycle ratio, cycle time, data flow graphs, discrete event systems, experimental analysis, iteration bound, system performance analysis

15 Randomized instruction set emulation
Elena Gabriela Barrantes, David H. Ackley, Stephanie Forrest, Darko Stefanović
February 2005 **ACM Transactions on Information and System Security (TISSEC)**, Volume 8 Issue 1
Publisher: ACM Press
Full text available: pdf(374.44 KB) Additional Information: full citation, abstract, references, index terms

Injecting binary code into a running program is a common form of attack. Most defenses employ a "guard the doors" approach, blocking known mechanisms of code injection. *Randomized instruction set emulation* (RISE) is a complementary method of defense, one that performs a hidden randomization of an application's machine code. If foreign binary code is injected into a program running under RISE, it will not be executable because it will not know the proper randomization. The pape ...

Keywords: Automated diversity, randomized instruction sets, software diversity

16 Understanding fault-tolerant distributed systems
Flavin Cristian
February 1991 **Communications of the ACM**, Volume 34 Issue 2
Publisher: ACM Press
Full text available: pdf(6.17 MB) Additional Information: full citation, references, citings, index terms, review

17 Runtime specialization with optimistic heap analysis
Ajeet Shankar, S. Subramanya Sastry, Rastislav Bodík, James E. Smith
October 2005 **ACM SIGPLAN Notices , Proceedings of the 20th annual ACM SIGPLAN conference on Object oriented programming systems languages and applications OOPSLA '05**, Volume 40 Issue 10
Publisher: ACM Press
Full text available: pdf(425.12 KB) Additional Information: full citation, abstract, references, index terms

We describe a highly practical program specializer for Java programs. The specializer is powerful, because it specializes optimistically, using (potentially transient) constants in the heap; it is precise, because it specializes using data structures that are only partially invariant; it is deployable, because it is hidden in a JIT compiler and does not require any user annotations or offline preprocessing; it is simple, because it uses existing JIT compiler ingredients; and it is fast, because ...

Keywords: dynamic optimization, partial evaluation, program analysis, specialization

18 Computer security (SEC): Unsupervised learning techniques for an intrusion detection system
Stefano Zanero, Sergio M. Savaresi
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**
Publisher: ACM Press
Full text available: pdf(337.99 KB) Additional Information: full citation, abstract, references, index terms

With the continuous evolution of the types of attacks against computer networks, traditional intrusion detection systems, based on pattern matching and static signatures, are increasingly limited by their need of an up-to-date and comprehensive knowledge base. Data mining techniques have been successfully applied in host-based intrusion detection. Applying data mining techniques on raw network data, however, is made difficult by the sheer size of the input; this is usually avoided by discarding ...

Keywords: K-means, anomaly detection, intrusion detection, principal direction divisive partitioning, quality of clusters, self-organizing maps, unsupervised clustering

19 Frontmatter (TOC, Letters, Election results, Software Reliability Resources!, Computing Curricula 2004 and the Software Engineering Volume SE2004, Software Reuse Research, ICSE 2005 Forward)
July 2005 **ACM SIGSOFT Software Engineering Notes**, Volume 30 Issue 4
Publisher: ACM Press
Full text available: pdf(6.19 MB) Additional Information: full citation, index terms

20 Special section on data mining for intrusion detection and threat analysis: Data mining-based intrusion detectors: an overview of the columbia IDS project
Salvatore J. Stolfo, Wenke Lee, Philip K. Chan, Wei Fan, Eleazar Eskin
December 2001 **ACM SIGMOD Record**, Volume 30 Issue 4
Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player